**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF TEXAS**
**SHERMAN DIVISION**

| | |
|---|---|
| ANCORA TECHNOLOGIES, INC.,<br><br>Plaintiff,<br><br>v.<br><br>TCL CORP.;<br>TCL COMMUNICATION LTD.;<br>TCL COMMUNICATION TECHNOLOGY HOLDINGS LTD.;<br>TCT MOBILE INTERNATIONAL LTD.;<br>TCT MOBILE, INC.; TCT MOBILE (US) INC.; AND TCT MOBILE (US) HOLDINGS INC.,<br><br>Defendants. | Case No. 4:19-cv-00624-ALM<br><br>DEMAND FOR JURY TRIAL |

# AMENDED COMPLAINT FOR PATENT INFRINGEMENT AND DEMAND FOR JURY TRIAL

Plaintiff, ANCORA TECHNOLOGIES, INC. ("Ancora"), for its Amended Complaint against TCL Corp., TCL Communication Ltd., TCL Communication Technology Holdings Ltd., TCT Mobile International Ltd., TCT Mobile Inc., TCT Mobile (US) Inc., TCT Mobile (US) Holdings Inc., (collectively "TCL") herein, states as follows:

## I. THE PARTIES

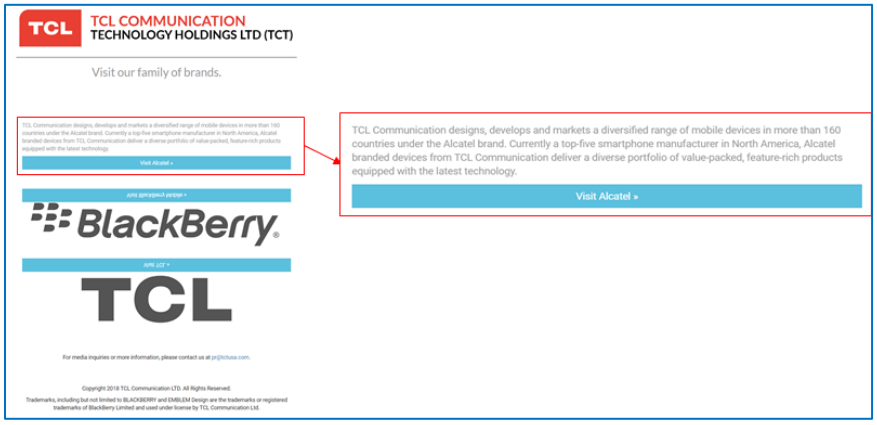
1. Plaintiff Ancora Technologies, Inc. is a corporation organized and existing under the laws of the State of Delaware and having a place of business at 23977 S.E. 10th Street, Sammamish, Washington 98075.

2. Upon information and belief, TCL Corp. is a corporation duly organized and existing under the laws of the People's Republic of China, having an address of No. 26, the Third Road, Zhongkai Avenue, Huizhou City, Guangdong, P.R. China 516006.

3. Upon information and belief, TCL Communication Ltd. is a corporation duly organized and existing under the laws of the People's Republic of China, having an address of 7/F, Block F4, TCL International E City Zhong Shan Yuan Road, Nanshan District, Shenzhen China.

4. Upon information and belief, TCL Communication Technology Holdings Ltd. is a corporation duly organized and existing under the laws of the People's Republic of China, having an address of Block F4, TCL Communication Technology Building, TCL International E City, Zhong Shan Yuan Road, Nanshan District, Shenzhen, Guangdong, P.R. China, 518052.

5. Upon information and belief, TCL Communication Technology Holdings Ltd. is licensed to make, use, and sell Alcatel-branded mobile devices in the United States.




http://www.tctusa.com/

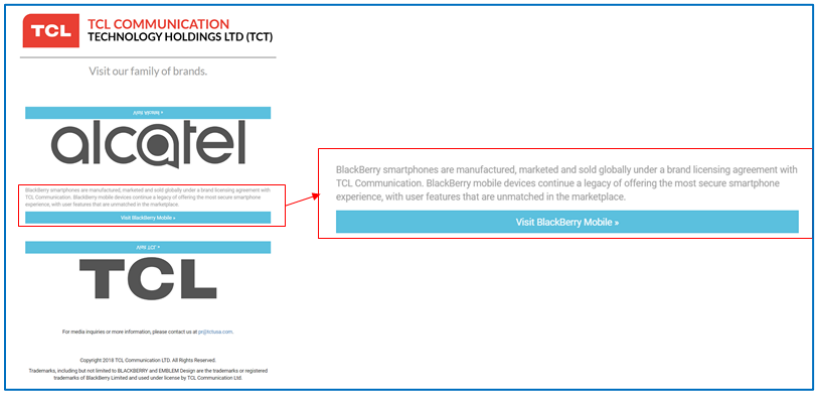
## ABOUT ALCATEL

TCL Communication Technology Holdings Limited (TCL Communication) designs, develops and markets a diversified range of mobile devices in more than 160 countries under the Alcatel brand. Currently a a top-10 global smartphone manufacturer, Alcatel branded devices from TCL Communication deliver innovative, feature-rich experiences that make access to today's mobile technology simple; offering a diverse portfolio of value-packed products equipped with the technology people want most.

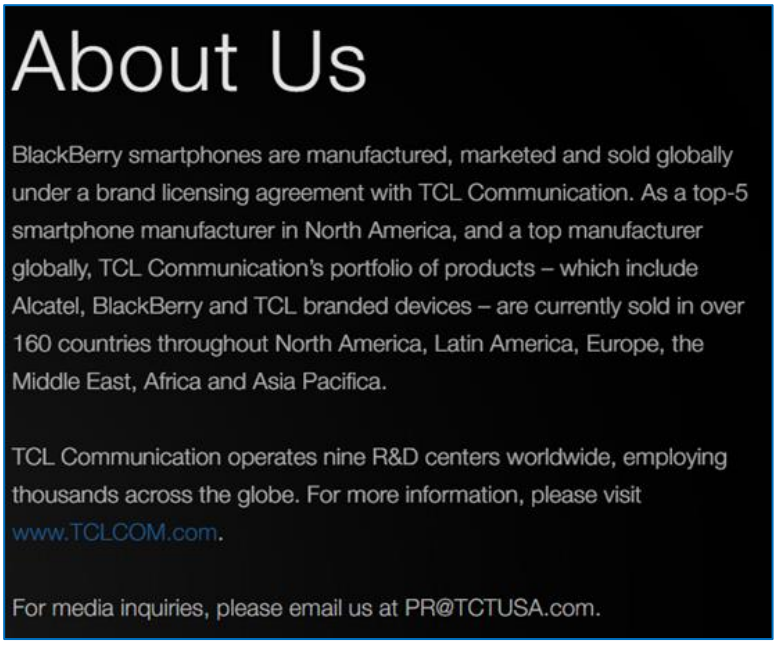
TCL Communication is a wholly owned company of TCL Corporation, one of the largest consumer electronics companies in the world. Alcatel is a trademark of Nokia used under license by TCL Communication.

https://us.alcatelmobile.com/about-us/

6. Upon information and belief, TCT is licensed to make, use, and sell Blackberry-branded mobile devices in the United States.




http://www.tctusa.com/




https://blackberrymobile.com/us/about-us/

7. Upon information and belief, TCT Mobile International Ltd. is a corporation duly organized and existing under the laws of the People's Republic of China, having an address of 5th Floor Building 22E No. 22 Science Park East Avenue, Hong Kong Science Park, Sha Tin, Hong Kong, China.

8. Upon information and belief, TCT Mobile, Inc. is a corporation existing under the laws of Delaware with its principle place of business at 25 Edelman, Suite 200, Irvine, California, 92618. TCT Mobile, Inc. may be served via its registered agent, Corporation Service Company, (d/b/a as CSC – Lawyers Incorporating Service), 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California, 95833.

9. Upon information and belief, TCT Mobile (US) Inc. is a corporation existing under the laws of Delaware with its principle place of business at 25 Edelman, Suite 200, Irvine, California, 92618. TCT Mobile (US) Inc. may be served via its registered agent, Corporation Service Company, (d/b/a as CSC – Lawyers Incorporating Service), 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California, 95833.

10. Upon information and belief, TCT Mobile (US) Holdings Inc. is a corporation existing under the laws of Delaware with its principle place of business at 25 Edelman, Suite 200, Irvine, California, 92618. TCT Mobile (US) Holdings Inc. may be served via its registered agent, Corporation Service Company, (d/b/a as CSC – Lawyers Incorporating Service), 2710 Gateway Oaks Drive, Suite 150N, Sacramento, California, 95833.

11. The Defendants identified in paragraphs 3-9 above are an interrelated group of companies which together comprise a manufacturer and seller of Android mobile devices in the United States, including Android mobile devices that are sold under the Alcatel and Blackberry brands.

## II. JURISDICTION

12. This is an action for infringement of United States patents arising under 35 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of the action under 28 U.S.C. § 1331 and § 1338(a).

13. This Court has personal jurisdiction over Defendants pursuant to due process and/or the Texas Long Arm Statute because, *inter alia*, (i) Defendants have done and continue to do business in Texas and (ii) Defendants have committed and continue to commit acts of patent

infringement in the State of Texas, including making, using, offering to sell, and/or selling accused products in Texas, and/or importing accused products into Texas, including by Internet sales and sales via retail and wholesale stores, inducing others to commit acts of patent infringement in Texas, and/or committing a least a portion of any other infringements alleged herein. In addition, or in the alternative, this Court has personal jurisdiction over Defendants pursuant to Fed. R. Civ. P. 4(k)(2).

14. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b), 1391(c), and 1400(b) because (i) Defendants have done and continue to do business in this district; (ii) Defendants have committed and continue to commit acts of patent infringement in this district, including making, using, offering to sell, and/or selling accused products in this district, and/or importing accused products into this district, including by internet sales and sales via retail and wholesale stores, and/or inducing others to commit acts of patent infringement in this district; and (iii) Defendants are foreign entities.

15. Venue is proper as to Defendants, which are organized under the laws of the People's Republic of China, Hong Kong, and Canada. 28 U.S.C. § 1391(c)(3) provides that "a defendant not resident in the United States may be sued in any judicial district, and the joinder of such a defendant shall be disregarded in determining where the action may be brought with respect to other defendants."

## III. BACKGROUND

16. On June 25, 2002, U.S. Patent No. 6,411,941 ("the '941 patent") entitled "Method Of Restricting Software Operation Within A License Limitation" was duly and legally issued. (*See* Exhibit A, U.S. Patent No. 6,411,941.) A reexamination certificate also issued to the '941 patent on June 1, 2010 where the patentability of all claims was confirmed by the United States Patent Office. (Exhibit B, *Ex Parte* Reexamination Certificate Issued Under 35 U.S.C. § 307.)

17. The ’941 patent has been involved in litigation against Microsoft Corporation, Dell Incorporated, Hewlett Packard Incorporated, and Toshiba America Information Systems. (*See* 2009-cv-00270, Western District of Washington.)

18. The ’941 patent has also been involved in litigation against Apple Incorporated. (*See* 2015-cv-03659, Northern District of California.)

19. The ’941 patent is currently involved in litigation against HTC America, Inc. and HTC Corporation. (*See* 2016-cv-01919, Western District of Washington.)

20. The ’941 patent is currently involved in litigation against Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (*See* 2019-cv-00385, Western District of Texas.)

21. The ’941 patent is currently involved in litigation against LG Electronics USA, Inc. and LG Electronics, Inc. (*See* 2019-cv-00384, Western District of Texas.)

22. The ’941 patent was involved in a Covered Business Method proceeding before the U.S. Patent and Trademark Office (*See* PTAB-CBM2017-00054). The U.S. Patent and Trademark Office denied institution of the petition filed by HTC and found the ’941 patent recites a “technological improvement to problems arising in prior art software and hardware methods of restricting an unauthorized software program’s operation.” (*See* PTAB-CBM2017-00054, Paper No. 7 at pg. 9.)

23. The U.S. Court of Appeals for the Federal Circuit further issued an order on November 16, 2018 regarding the validity of the ’941 patent. (*See* CAFC 18-1404, Dkt. # 39.) In this appeal, the U.S. Court of Appeals for the Federal Circuit held:

> [T]he claimed invention moves a software-verification structure to a BIOS location not previously used for this computer-security purpose and alters how the function is performed (in that the BIOS memory used for verification now interacts with distinct computer memory to perform a software-verification function), yielding a tangible technological benefit (by making the claimed system less susceptible to hacking).

CAFC 18-1404, Dkt. #39, pg. 13.

24. The U.S. Court of Appeals for the Federal Circuit further issued an order on March 3, 2014 regarding claim construction and invalidity of the '941 patent. (*See* CAFC 13-1378, Dkt. #57.)

25. Ancora is the owner of all right, title and interest in the '941 patent.

## IV. COUNT I – PATENT INFRINGEMENT

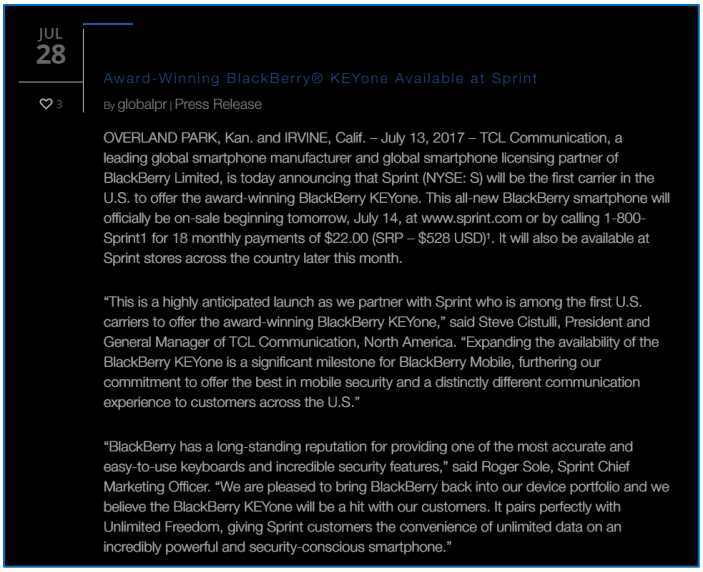
26. Ancora realleges the preceding paragraphs as though set forth fully herein.

27. TCL has infringed the '941 patent in violation of 35 U.S.C. § 271(a) by, prior to the expiration of the '941 patent, selling, and/or offering for sale in the United States, and/or importing into the United States, without authorization, products that are capable of performing at least Claim 1 of the '941 patent literally or under the doctrine of equivalents and/or, without authorization, causing products to perform each step of at least Claim 1 of the '941 patent.

28. Accused Products include, but are not limited to, the Alcatel 3c/33x/3v/3L; Alcatel 1c/1x/1/1t7/1T10; Alcatel A3/A3XL/A7XL/A7/A2XL/A3A; Alcatel A5; Alcatel IDOL 4/4S/5; Alcatel POP 4/4S/4PLUS; Alcatel PIXI 4(4)/4(5)/4(6); Blackberry KeyONE; and Blackberry Key2 ("Accused Products").

29. Upon information and belief, TCL began selling the accused Alcatel products between 2016 - 2018.

30. Upon information and belief, TCL began selling the Blackberry KeyONE in 2017.



JUL
28

♡ 3

Award-Winning BlackBerry® KEYone Available at Sprint

By globalpr | Press Release

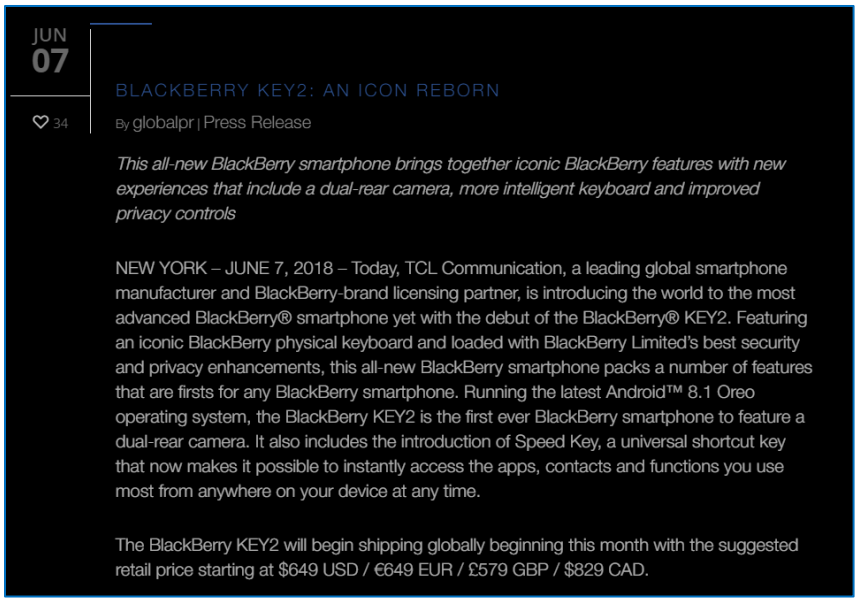
OVERLAND PARK, Kan. and IRVINE, Calif. – July 13, 2017 – TCL Communication, a leading global smartphone manufacturer and global smartphone licensing partner of BlackBerry Limited, is today announcing that Sprint (NYSE: S) will be the first carrier in the U.S. to offer the award-winning BlackBerry KEYone. This all-new BlackBerry smartphone will officially be on-sale beginning tomorrow, July 14, at www.sprint.com or by calling 1-800-Sprint1 for 18 monthly payments of $22.00 (SRP – $528 USD)[1]. It will also be available at Sprint stores across the country later this month.

"This is a highly anticipated launch as we partner with Sprint who is among the first U.S. carriers to offer the award-winning BlackBerry KEYone," said Steve Cistulli, President and General Manager of TCL Communication, North America. "Expanding the availability of the BlackBerry KEYone is a significant milestone for BlackBerry Mobile, furthering our commitment to offer the best in mobile security and a distinctly different communication experience to customers across the U.S."

"BlackBerry has a long-standing reputation for providing one of the most accurate and easy-to-use keyboards and incredible security features," said Roger Sole, Sprint Chief Marketing Officer. "We are pleased to bring BlackBerry back into our device portfolio and we believe the BlackBerry KEYone will be a hit with our customers. It pairs perfectly with Unlimited Freedom, giving Sprint customers the convenience of unlimited data on an incredibly powerful and security-conscious smartphone."

https://blackberrymobile.com/press-room/

31. Upon information and belief, TCL began selling the Blackberry Key2 in 2018.



JUN
07

♡ 34

BLACKBERRY KEY2: AN ICON REBORN

By globalpr | Press Release

*This all-new BlackBerry smartphone brings together iconic BlackBerry features with new experiences that include a dual-rear camera, more intelligent keyboard and improved privacy controls*

NEW YORK – JUNE 7, 2018 – Today, TCL Communication, a leading global smartphone manufacturer and BlackBerry-brand licensing partner, is introducing the world to the most advanced BlackBerry® smartphone yet with the debut of the BlackBerry® KEY2. Featuring an iconic BlackBerry physical keyboard and loaded with BlackBerry Limited's best security and privacy enhancements, this all-new BlackBerry smartphone packs a number of features that are firsts for any BlackBerry smartphone. Running the latest Android™ 8.1 Oreo operating system, the BlackBerry KEY2 is the first ever BlackBerry smartphone to feature a dual-rear camera. It also includes the introduction of Speed Key, a universal shortcut key that now makes it possible to instantly access the apps, contacts and functions you use most from anywhere on your device at any time.

The BlackBerry KEY2 will begin shipping globally beginning this month with the suggested retail price starting at $649 USD / €649 EUR / £579 GBP / $829 CAD.

https://blackberrymobile.com/press-room/

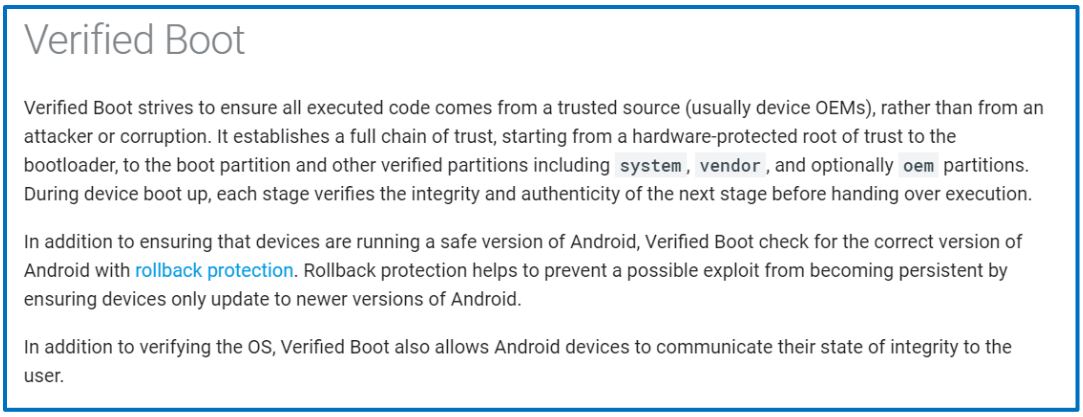
32. At a minimum, the Accused Products include servers/software utilized by TCL to transmit an over-the-air ("OTA") software update, as well as those smartphones and other

devices and technology that received from TCL, or received at TCL's direction, an OTA update that caused such device to perform the method recited in Claim 1 prior to the expiration of the '941 patent.

33. Such Accused Products are configured by TCL such that they are capable of performing each step of Claim 1 of the '941 patent and to which TCL provided one or more OTA updates before the expiration of the '941 patent that would cause a TCL device to perform each step of Claim 1 in order to upgrade its operating system. (*See e.g.*, https://www.att.com/devicehowto/tutorial.html#!/stepbystep/id/stepbystep_KM1231051?make=BlackBerry&model=BBB100&gsi=mpo8f8; https://support.sprint.com/support/pages/printTemplate.jsp?articleId=WServiceAdvisory_542_GKB92134-dvc9760001prd.)

34. For example, Claim 1 of the '941 patent claims "a method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of: [1] selecting a program residing in the volatile memory, [2] using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record, [3] verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and [4] acting on the program according to the verification."

35. When TCL transmitted an OTA update, TCL performed and/or caused to be performed each of these elements as part of what is described as "verified boot":



## Verified Boot

Verified Boot strives to ensure all executed code comes from a trusted source (usually device OEMs), rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader, to the boot partition and other verified partitions including `system`, `vendor`, and optionally `oem` partitions. During device boot up, each stage verifies the integrity and authenticity of the next stage before handing over execution.

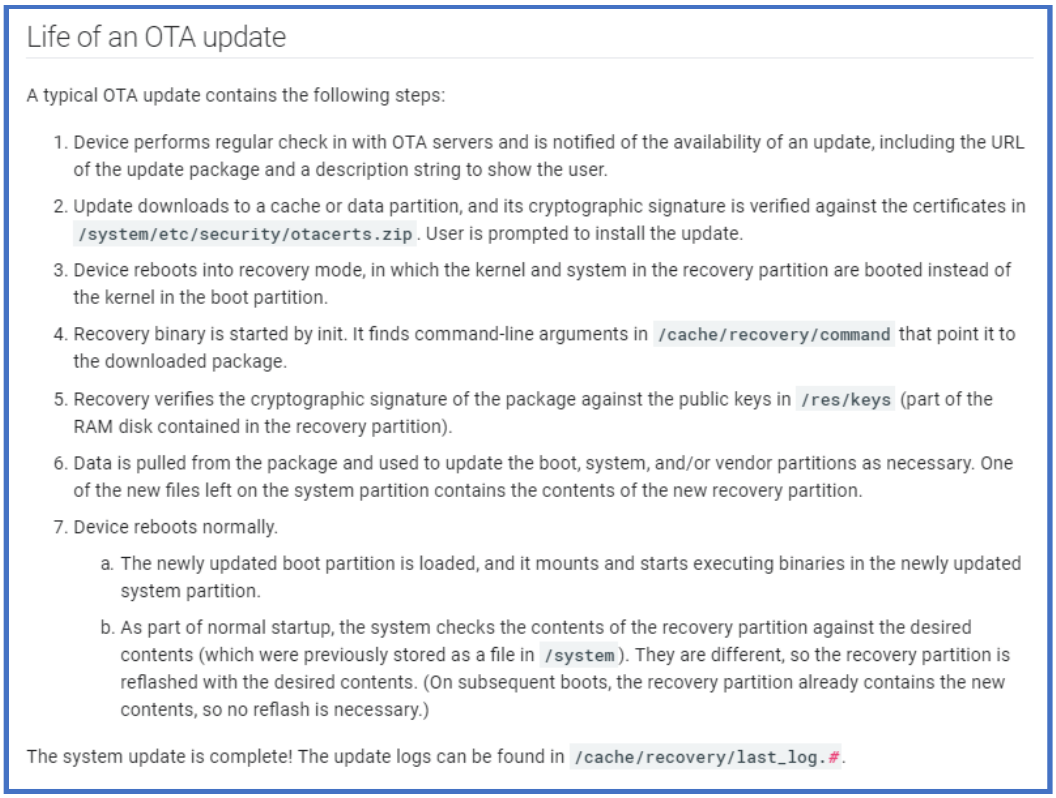
In addition to ensuring that devices are running a safe version of Android, Verified Boot check for the correct version of Android with rollback protection. Rollback protection helps to prevent a possible exploit from becoming persistent by ensuring devices only update to newer versions of Android.

In addition to verifying the OS, Verified Boot also allows Android devices to communicate their state of integrity to the user.

https://source.android.com/security/verifiedboot

36. In particular, each mobile device contains both erasable, non-volatile memory in the form of ROM and volatile memory in the form of RAM.

37. Further, each mobile device was configured by TCL to perform the below described process (or one substantially like it) in order to install an OTA update:



## Life of an OTA update

A typical OTA update contains the following steps:

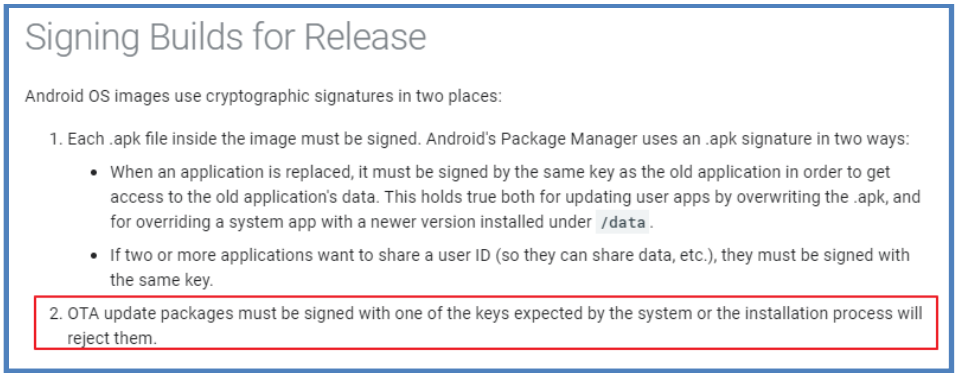
1. Device performs regular check in with OTA servers and is notified of the availability of an update, including the URL of the update package and a description string to show the user.
2. Update downloads to a cache or data partition, and its cryptographic signature is verified against the certificates in `/system/etc/security/otacerts.zip`. User is prompted to install the update.
3. Device reboots into recovery mode, in which the kernel and system in the recovery partition are booted instead of the kernel in the boot partition.
4. Recovery binary is started by init. It finds command-line arguments in `/cache/recovery/command` that point it to the downloaded package.
5. Recovery verifies the cryptographic signature of the package against the public keys in `/res/keys` (part of the RAM disk contained in the recovery partition).
6. Data is pulled from the package and used to update the boot, system, and/or vendor partitions as necessary. One of the new files left on the system partition contains the contents of the new recovery partition.
7. Device reboots normally.
    a. The newly updated boot partition is loaded, and it mounts and starts executing binaries in the newly updated system partition.
    b. As part of normal startup, the system checks the contents of the recovery partition against the desired contents (which were previously stored as a file in `/system`). They are different, so the recovery partition is reflashed with the desired contents. (On subsequent boots, the recovery partition already contains the new contents, so no reflash is necessary.)

The system update is complete! The update logs can be found in `/cache/recovery/last_log.#`.

https://source.android.com/devices/tech/ota/nonab

38. For example, during this process, a program running on one or more OTA servers owned and/or controlled by TCL set up a verification structure in the erasable, non-volatile memory of the BIOS of the Accused Products by transmitting to the device an OTA update. The Accused Products are then configured by TCL to save to a partition (*e.g.*, the "cache" or "A/B" partitions) of the erasable, non-volatile memory of its BIOS.

39. The OTA update contains a verification structure that include data accommodating at least one license record. Examples of such a license record include a cryptographic signature or key:



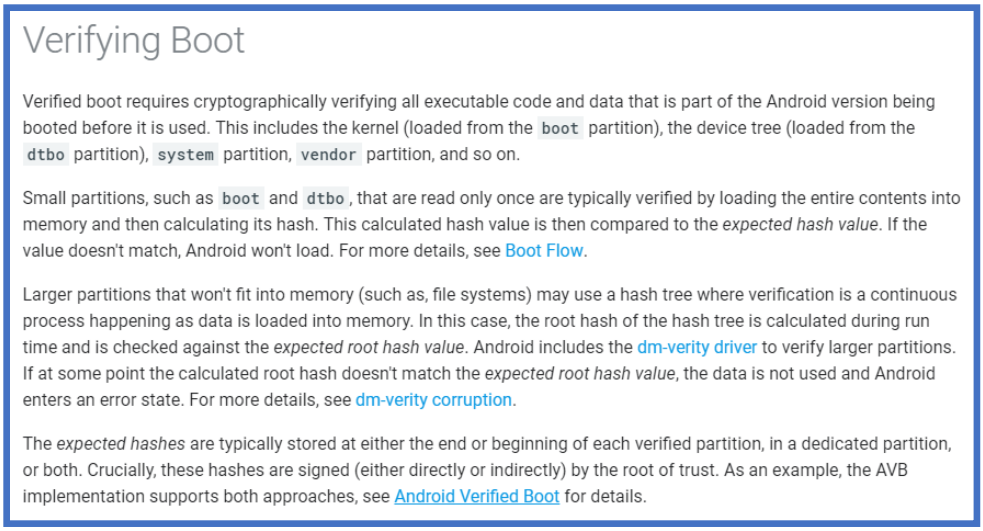
Signing Builds for Release

Android OS images use cryptographic signatures in two places:

1. Each .apk file inside the image must be signed. Android's Package Manager uses an .apk signature in two ways:
   - When an application is replaced, it must be signed by the same key as the old application in order to get access to the old application's data. This holds true both for updating user apps by overwriting the .apk, and for overriding a system app with a newer version installed under `/data`.
   - If two or more applications want to share a user ID (so they can share data, etc.), they must be signed with the same key.
2. OTA update packages must be signed with one of the keys expected by the system or the installation process will reject them.

https://source.android.com/devices/tech/ota/sign_builds

40. Such license record also may comprise a cryptographic hash or hash tree:



Verifying Boot

Verified boot requires cryptographically verifying all executable code and data that is part of the Android version being booted before it is used. This includes the kernel (loaded from the `boot` partition), the device tree (loaded from the `dtbo` partition), `system` partition, `vendor` partition, and so on.

Small partitions, such as `boot` and `dtbo`, that are read only once are typically verified by loading the entire contents into memory and then calculating its hash. This calculated hash value is then compared to the *expected hash value*. If the value doesn't match, Android won't load. For more details, see Boot Flow.

Larger partitions that won't fit into memory (such as, file systems) may use a hash tree where verification is a continuous process happening as data is loaded into memory. In this case, the root hash of the hash tree is calculated during run time and is checked against the *expected root hash value*. Android includes the dm-verity driver to verify larger partitions. If at some point the calculated root hash doesn't match the *expected root hash value*, the data is not used and Android enters an error state. For more details, see dm-verity corruption.

The *expected hashes* are typically stored at either the end or beginning of each verified partition, in a dedicated partition, or both. Crucially, these hashes are signed (either directly or indirectly) by the root of trust. As an example, the AVB implementation supports both approaches, see Android Verified Boot for details.

https://source.android.com/security/verifiedboot/verified-boot.

41. Once the verification structure has been set up in the BIOS, the Accused Products are configured by TCL to reboot into recovery mode, load the OTA update into its volatile memory (e.g., RAM), and use the at least one license record from the BIOS to verify the OTA update.

42. If the OTA update is verified, the Accused Products are configured to load and execute the update.

43. In sum, as described above, once TCL has set up the verification structure by transmitting to a device an OTA update, each Accused Product is configured to automatically perform each of the remaining Claim 1 steps.

44. Further, on information and belief, when TCL provided OTA updates, TCL performed or caused to be performed each of the Claim 1 steps.

45. Further, TCL conditions participation in the OTA update process and the receipt of the benefit of a software update on the performance of each of the above steps.

46. Primarily, as described above, TCL pre-configures/programs each Accused Product to perform the above described steps upon receiving an OTA update from TCL.

47. Further, TCL takes steps to ensure that each Accused Product cannot install an OTA update except by performing each of the above described steps.

48. Further, TCL emphasizes the benefits associated with updating the software of its Accused Products.

49. Further, TCL controlled the manner of the performance of such method. As set forth above, TCL configured each Accused Product such that, upon receiving an OTA update, it would automatically perform each remaining step of the claimed method.

50. TCL also controlled the timing of the performance of such method by determining when to utilize its OTA servers/software to set up a verification structure in each Accused Product.

51. TCL also had the right and ability to stop or limit infringement simply by not performing the initial step of using its OTA servers/software to set up a verification structure in each Accused Product. Absent this action by TCL, the infringement at issue would not have occurred.

52. TCL's infringement has caused damage to Ancora, and Ancora is entitled to recover from TCL those damages Ancora has sustained as a result of TCL's infringement.

## V. DEMAND FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. Declaring that TCL has infringed United States Patent No. 6,411,941 in violation of 35 U.S.C. § 271;

B. Awarding damages to Ancora arising out of this infringement, including enhanced damages pursuant to 35 U.S.C. § 284 and prejudgment and post-judgment interest, in an amount according to proof;

C. Awarding such other costs and relief the Court deems just and proper, including any relief that the Court may deem appropriate under 35 U.S.C. § 285.

## VI. DEMAND FOR JURY TRIAL

Ancora respectfully demands a trial by jury of any and all issues triable of right by a jury in the above-captioned action.

Respectfully submitted,

Dated: September 12, 2019

/s/ Marc Lorelli

Marc Lorelli (MI Bar No. P63156) LEAD COUNSEL
Mark A. Cantor (MI Bar No. P32661)
John S. LeRoy (MI Bar No. P61964)
John P. Rondini (MI Bar No. P72254)
**BROOKS KUSHMAN P.C.**
1000 Town Center, Twenty-Second Floor
Southfield, Michigan 48075

Telephone: (248) 358-4400
Facsimile: (248) 358-3351
Email: mlorelli@brookskushman.com
mcantor@brookskushman.com
jleroy@brookskushman.com
jrondini@brookskushman.com

**SIEBMAN FORREST BURG & SMITH, LLP**
Clyde M. Siebman – TX State Bar #18341600
clydesiebman@siebman.com
Elizabeth S. Forrest – TX State Bar #24086207
elizabethforrest@siebman.com
Federal Courthouse Square
300 N. Travis
Sherman, TX 75090
(903) 870-0070
(903) 870-0066 Telefax

*Attorneys for Ancora Technologies, Inc.*

**CERTIFICATE OF SERVICE**

I hereby certify that a copy of the foregoing document was filed electronically in compliance with Local Rule CV-5(a). Therefore, this document was served on all counsel who are deemed to have consented to electronic service. Local Rule CV-5(a)(3)(A). Pursuant to Fed. R. Civ. P. 5(d) and Local Rule CV-5(d) and (e), all other counsel of record not deemed to have consented to electronic service were served with a true and correct copy of the foregoing by email on September 12, 2019.

*/s/ Marc Lorelli*